NEBRASKA AUDITOR OF PUBLIC ACCOUNTS

Mike Foley
State Auditor

Mike.Foley@apa.ne.gov
P.O. Box 98917
State Capitol, Suite 2303
Lincoln, Nebraska 68509
402-471-2111, FAX 402-471-3301
www.auditors.state.ne.us

November 24, 2008

Brenda Decker
Chief Information Officer
Office of the Chief Information Officer
501 S. 14th Street
P.O. Box 95045
Lincoln, NE 68509

Dear Brenda:

The Auditor of Public Accounts (APA) has completed our examination of information technology (IT) internal control procedures for select applications for the fiscal year ending June 30, 2008. These systems support financial reporting and disclosure for the State of Nebraska.

The design and operating effectiveness of applicable computer controls were tested through internal control procedures. We discussed, confirmed, and observed controls with each respective agency's management. The procedures performed related to computer operations, information security, and change management consisting of a combination of inquiry, corroboration, observation, and re-performance. Interfaces significant to financial reporting were also selected for testing.

The specific confidential details and information were provided separately to agency's management and your office. The following is a high-level overview of the applications included in our testing.

Department of Administrative Services (DAS):

- ***Nebraska Information System (NIS)*** - This application is responsible for processing the financial, human resource, and procurement data business processes for the State of Nebraska. There are extensive interfaces with other state applications.
- ***Communications Service Billing (CSB)*** - This application tracks the phone use charges for each State agency.
- ***PACE*** **–** This third party product reads IBM mainframe log files used by agencies for billing purposes.

Department of Health & Human Services (DHHS):

- ***Children Have a Right to Support (CHARTS)*** - CHARTS is used for statewide Child Support Enforcement (CSE). Processes include case initiation, location, establishment, case management, enforcement, financial management, and state/federal reporting. There are extensive interfaces with other state and federal organizations.
- ***Nebraska Family Online Client User System (NFOCUS) –*** The NFOCUS application is used to automate benefit/service delivery and case management for over 30 DHHS programs. NFOCUS processes include client/case intake, eligibility determination, case management, service authorization, benefit payments, claims processing and payments, provider contract management, interfacing with other state and federal organizations, and management and government reporting.
- ***Medicaid Management Information System (MMIS) –*** This application supports the operation of the Medicaid program which is federally-regulated, state-administered, and provides medical care and services. The objective of MMIS is to improve and expedite claims processing, efficiently control program costs, effectively increase the quality of services, and examine cases of suspected program abuse.
- ***Home Energy Assistance (HEA) –*** This application supports the federally funded Low Income Energy Assistance Program (LIEAP). For qualified households, the Home Energy application stores the case information and generates energy assistance payments to both clients and providers.
- ***Woman Infants and Children (WIC)*** - This application is used to determine client eligibility and to print food instruments for the Special Supplemental Nutrition Program for Women, Infants, and Children (WIC).
- ***Automated Computer Tracking System (ACTS)*** - The ACTS application supports the Every Woman Matters and Wise Woman Programs. These programs are federally funded by the Center for Disease Control and Prevention (CDCP). They provide breast and cervical cancer and cardiovascular and diabetes screening to women ages 40-64. The application is used to determine program eligibility, manage client health records, calculate payments to providers and create reports for CDCP.

Nebraska Department of Education (NDE):

- ***Grants Management System (GMS) –*** This application is used by outside users to apply for grant funds and by NDE to approve and process payments for grant funds. Grant payments made to pre-selected school districts are interfaced with NIS through a separate process.
- ***Quality Employment Solutions through Teams (QUEST)*)** – QUEST is utilized by Vocational Rehabilitation staff to track all expenses paid to assist physically and/or mentally disabled persons in locating jobs. It includes aid to complete school, help purchase dress clothes, set up interviews, etc.
- ***Disability Determination System (DDS) –*** The application serves as a customer resource manager and information tracking system for payments to medical practitioners for information they provide to the social security administration pertaining to pending disability claims.

Department of Labor (Labor):

- ***Tax Management System (TMS)*** – TMS records daily transactions regarding employer Unemployment Insurance (UI) accounts.
- ***Benefits Payment System (BPS)*** – This application processes payments to eligible claimants for unemployment insurance and accounts for all overpayment collection activities.

Nebraska Public Employees Retirement System (NPERS):

- ***Pension Information of Nebraska for Efficient and Effective Retirement (PIONEER)* –** The PIONEER application processes contributions from members and employers and prepares information for NIS to print member benefit payments.

Department of Revenue:

- ***Tax Processing Applications*** – The Department of Revenue utilizes multiple tax processing applications. These tax applications include, but are not limited to the processing of: sales tax, corporate and individual income tax, fiduciary tax, motor fuels tax, motorboat tax and fees, cigarette tax, waste reduction and recycling fees, tire fees, litter fees, lodging tax, and drug tax. Additional applications track and process charitable gaming licenses, Homestead Exemption for property tax, fertilizer fee systems, and the partnership system.
- ***NebFile*** - The NebFile application allows Nebraska resident taxpayers to file their state income tax return free over the Internet. NebFile is not tax preparation software, but will do simple calculations and table look-ups for the taxpayer. The NebFile system allows individuals to file a short form, Form 1040NS, or a long form, 1040N, with some limitations.

Department of Roads:

- ***Project Finance Systems (PFS)* –** Surface transportation projects are managed by PFS.
- ***Maintenance Management System (MMS)* –** MMS manages labor, equipment, materials, maintenance contracts, and indirect costs for routine highway maintenance.
- ***Roads Payment System (RPS)* –** Department of Roads utilizes RPS to process payments to vendors.

Department of Motor Vehicles:

- ***Vehicle Title Registration (VTR)*** - VTR is an application developed by the Department of Motor Vehicles to provide an overall system to be utilized by the counties in vehicle titling and registration. It is a statutory requirement for all counties in the State to utilize this system.

State Treasurer:

- ***KidCare*** - The KidCare application supports child support payment processing, including receipt and disbursement for nearly 100,000 child support payments to custodial parents each month.
- ***Wagers*** - The Wagers application maintains information regarding unclaimed property remitted to the State of Nebraska and pays claims for specific property held.

Nebraska Lottery:

- ***Internal Control System (ICS)*** – ICS independently validates and balances the online and instant games system results.
- ***LOTeries Operating System (LOTOS)*** **–** LOTOS operates the online gaming services.
- ***Instant Processing System (IPS)*** **–** IPS operates the scratch/instant gaming services.

In connection with the examination described above, we noted certain matters involving internal controls over information technology which are presented below for your consideration. These comments and recommendations, which have been discussed with appropriate agencies independently and in detail, are intended to improve the internal controls over information technology.

It should be noted this letter is critical in nature since it contains only our comments and recommendations on the areas noted for improvement.

COMMENTS AND RECOMMENDATIONS

1. Segregation of Duties

Access to system resources is determined by certain access privileges granted to a user. In order to retain appropriate segregation of duties, an agency should grant employees adequate system access to perform their job responsibility and prevent unauthorized access. Changes to an employee's role or responsibility may require a change in the access privileges associated with his or her user id.

- Twenty-eight State employees with NIS daily processing access had the ability to create and approve their own accounting entries. DAS is in the process of fully implementing a NIS integrity report to list voucher batches created and posted by the same NIS ID. The report will be reviewed by the State Accounting Division for further follow-up. The integrity report focuses on voucher batches only and does not include any other batch types within NIS.
- The State Treasurer - Unclaimed Property Division had three staff which were assigned multiple database roles and substantial access rights to Wagers. No compensating controls were in place to reasonably reduce the risk of fraud.
- Sixty-two employees at the Labor had the ability to prepare and approve claims within the BPS application in the prior fiscal year. A similar number of employees still had the ability to prepare and approve claims within the BPS application for the current fiscal year. During the fiscal year, Labor developed and generated a report that determines who prepared and approved the claim within BPS, which is to be reviewed quarterly. Labor conducted its first review of the report in April 2008, which meant that at lease half of the fiscal year did not have a compensating control in place to monitor employees with the dual access were appropriate.
- A similar finding was noted in our prior IT audit work.

An individual with the ability to both prepare and approve accounting transactions in an application increases the risk of unintended or unauthorized transactions being processed.

Employees with this type of access can process financial transactions without anyone else's knowledge or involvement. As a result, unapproved or inaccurate payments could be made.

> We recommend a user's ability to both initiate and approve transactions be eliminated when possible. System access should be segregated so the same user cannot perform both functions in an application. If this level of access is necessary to perform job functions, an independent review should occur on a continuous basis to ensure transactions prepared and approved by the same person are appropriate and correct.

2. Developer Access to Production Environment

Access to information resources should be restricted based upon job responsibilities to help enforce proper segregation of duties and reduce the risk of unauthorized system access. Programmers should generally be limited to accessing only the information specifically required to complete their assigned systems development projects and expressly prohibited from directly accessing production software and data information. Computer operators normally should be permitted to run production jobs; however, they should be restricted from accessing the development environment. Access to production program libraries and data information should be logged and periodically reviewed for appropriateness.

- Two NIS application developers maintained access to the server environment and the supporting database. This finding was noted in the prior IT audit.
- Two application developers at the State Treasurer's office had administrator access to the Windows environment and to the KidCare application's database. The application developers also had administrative access to the KidCare application. This was a prior year finding; however, based on the size of the IT department, management has accepted the risk.
- NDE had three contracted developer IDs, two Application Developer IDs, and two unassigned IDs that had super user access to GMS database(s). One of the contractor IDs had server wide access to the SQL server which the GMS database resides on.
- NDE had Quest application developers, two DDS application developers, and one Social Security Administration DDS contracted developer with access to their respective production environments.
- Department of Revenue application developers had the ability to develop and promote changes to production in the GPS, Homestead Exemption, Motor Fuels, Charitable Gaming, and Motorboat applications. This finding was noted in the prior IT audit.

Application developers with access to the database and the production environment have the ability to circumvent the standard change control process and implement modifications that may not be consistent with management's intentions.

> Depending on the size of the information technology department, developers may need access to the production processing environment. In order to mitigate the risk of moving unintended

changes into production, compensating controls should be established. We recommend developers be required to obtain approval prior to moving changes into production. In addition, a compensating control such as review of audit logs or automatic notification should be established to identify all changes made to the production environment.

3. Access Commensurate with Job Responsibilities

Users improperly granted the ability to make changes to system security parameters may result in unapproved changes being implemented. Unauthorized modifications to job scheduling software may result in unauthorized, incomplete, or inaccurate processing. If such access is not implemented and configured properly, business cycle controls may be ineffective. When users are granted access that is not commensurate with their job responsibilities, significant information resources may be modified inappropriately, disclosed without authorization, and/or unavailable when needed.

- Two NIS application developers had authority within the AS/400, which was not required as part of their daily job responsibility.
- Based upon job responsibilities, one of eight NIS users with statewide payroll update access did not require the access.
- The State Treasurer’s Wagers Unclaimed Property Application allows users to forcefully balance a report that is not in balance. Six users were assigned access to the tool to forcefully balance a report including a terminated user. Of these six users, three had the necessary database roles to actually use the tool not including the terminated employee.
- State Treasurer’s Unclaimed Property staff had the ability to both balance and unbalance reports within Wagers which allows them to modify unclaimed property claims. Additionally, during the fiscal year, the APA asked for two inquiry access user ids for Wagers. However, Unclaimed Property provided more than inquiry only access, which was subsequently corrected upon notification from the APA. These findings were both corrected as of May 30, 2008.
- NDE activation codes for employees with staff level access to the GMS application were the same for each user and not regularly changed. This finding was noted in the prior IT audit. Procedures have not been established to document a review of the staff level access to ensure only authorized individuals had access to GMS.
- Twenty-four DHHS users were identified with access to sensitive NFOCUS and CHARTS datasets who did not require this access to complete their job responsibilities. One DHHS user had the ability to make security setting changes and did not require the access as part of their job responsibilities. This finding was noted in the prior IT audit. Seven DHHS users had access to HEA production datasets who did not require this access to complete their job responsibilities.
- The Department of Revenue was performing a review of users with access to mainframe applications; however, only user id’s inactive for two or more years were removed. The Department of Revenue did not document the review of network user access. In addition, one user was given access to the Motor Fuels application; however, there was no documentation to support the access.

Without a proper segregation of duties, programmers or system administrators have the capability to create and approve unauthorized changes if they choose to do so. When an individual has access not required by their job duties, there is an increased risk for the loss of State funds due to error or fraud. There is also a risk that unauthorized transactions or changes could occur. Without periodically changing the activation codes allowing access to an application, there is an increased risk users may gain unauthorized access through the utilization of a single access code.

> We recommend all application owners review a list of their users and verify access levels are accurate. This should be done on a periodic basis to ensure access to the application is commensurate with employees' job responsibilities.

4. <u>Dataset Access</u>

Typically, entities restrict access to information resources (e.g., programs, data, networks) to enforce desired segregation of duties, facilitate on-line approvals, and help achieve business cycle control objectives. Logical security tools and techniques are used to define such access restrictions, including how and to whom the entity will limit the ability to view, use, or modify significant information resources.

- Labor application developers had access to production datasets for the Tax Management System application. Labor did not review database logs to ensure only appropriate changes were made. This finding was noted in the prior IT audit.
- DHHS application developers maintained access to production datasets for CHARTS, MMIS, and NFOCUS applications. Anywhere from one to six application developers for each application had ALTER access to production datasets. ALTER access allows users to read, update or change the datasets. This finding was noted in the prior IT audit. In addition, ten programmers/developers had ALTER access to HEA production datasets.
- Four application developers maintained access to the production datasets for the Corporate Income Tax and Individual Income Tax mainframe applications during the fiscal year. This finding was noted in the prior IT audit.

Without a proper segregation of duties, application developers could circumvent the change control process and modify the production environment without testing or obtaining management approval for changes. The resulting changes may lead to difficulties in maintaining system functions, processing errors, or inaccurate and misleading financial information.

> We recommend management evaluate potential options to restrict application developers' access to the production environment. In the event access restrictions are not feasible, monitoring controls should be implemented to ensure all modifications to production are appropriately approved and tested.

5. New and Terminated User Access

Changes to an employee's role or responsibility may require a change in the access privileges associated with a user id. These changes should be performed immediately upon the change of the employee's status. An employee’s system access should be immediately revoked upon termination.

- Four terminated individuals from the Department of Motor Vehicles, Labor, DHHS, and DAS had Resource Access Control Facility (RACF) ID’s with elevated privileges. RACF is a security system that provides access control and auditing functions for certain operating systems. An adequate review of RACF users was not performed to ensure access was reasonable. It was also noted the RACF auditor account had not accessed the mainframe in at least 60 days.
- Three of twelve users with NIS database access were terminated employees with active ids. A similar finding was noted in the prior IT audit.
- An employee who terminated on March 29, 2008 still had access to the State Treasurer’s Wagers application as of June 4, 2008.
- NDE did not have procedures to ensure GMS district administrator accounts were removed in a timely manner in the event of termination. Codes were not changed unless the district administrator specifically requested the action which could result in terminated employees registering again and transacting on the school districts grant. This finding was noted in the prior IT audit.
- Labor did not have appropriate procedures to ensure terminated users had their access removed in a timely manner. Labor also did not have appropriate procedures to ensure documentation of the access granted to new hires was maintained. Labor implemented a new form to address this finding in January 2008.
- DHHS did not have adequate documentation to support changes to security roles within the WIC application for 11 of 25 users tested. In addition, there was no documentation to support the removal of 2 of 2 terminated users from the ACTS application. Management does not document their review of users’ access to the ACTS application.

The identification and authentication of users validates the individuals who use computer systems. Inadequate approval of access or a lapse in removing access may lead to financial loss, operational damage through unintentional access, or deliberate unauthorized access. When access to networks and applications is not approved, terminated timely, or configured appropriately, it creates the opportunity for unauthorized processing of transactions.

> We recommend application owners review user access on a periodic basis to ensure access is appropriate. Additionally, a formalized process to grant and remove access to applications should be established and followed. Terminated users access should be removed immediately.

6. Shared IDs

Sharing of privileged IDs poses a threat to security because over time these user IDs and passwords may become known to individuals not intended to have this level of access. Individual user IDs should be used to validate use of the computer systems. A user ID distinguishes one user from another and establishes accountability for system-based actions.

- Eleven active RACF users with business/accounting job functions from DAS, Department of Motor Vehicles, Department of Corrections, and Nebraska Game and Parks Commission had "SPECIAL" attribute at the group level. A user with the "SPECIAL" attribute can execute any RACF security commands except the attributes specifically excluded within the system. It appeared agencies may have been sharing RACF IDs with elevated privileges.
- DHHS utilized four shared IDs with Domain Administrator privileges. Domain Administrators had the ability to make system and security changes. As of October 2007, the four shared IDs had been removed.
- DHHS utilized two shared user IDs with administrative privileges for the WIC application. The actions of the two IDs are logged within the system; however, no one reviews the logs. In addition, there were three shared user ID's for temporary workers with access to the WIC application. Unique IDs were not created due to the frequent turnover of student workers.
- DHHS utilized four shared IDs with access to an HEA production dataset. As of July 2008, DHHS is in the process of removing these shared IDs.
- NPERS had two accounts with Domain Administrator privileges on the database server which were shared among NPERS IT staff. Management has accepted the risk and has implemented procedures to monitor system logs and access. The current system does not allow for unique IDs to be implemented.

Inadequate authentication procedures may lead to financial loss and operational damage through unintentional or deliberate unauthorized access, alteration, and use of information resources. Shared ids make it difficult to identify the individual who accessed the computer system.

> We recommend eliminating all shared IDs to ensure individuals have a unique ID to make users accountable for transactions on computer systems.

7. Password Complexity

Passwords should be changed periodically and complexity of the length or types of passwords should be maintained at all times.

- Password complexity was enabled for the NIS AS/400; however, we noted certain issues including users not required to change their password, minimum password length was too short, and log-off/timeout function was too long. The NIS team is in the process of updating these password complexity changes.
- The State Treasurer's active directory password history was not set to industry password complexity standards. This finding was corrected in May 2008.

- The Department of Roads did not have password complexity requirements for the windows network. The Department of Roads implemented the Nebraska Information Technology Commission (NITC) standard for password complexity in May 2008.
- NDE GMS Portal passwords could be utilized for an unlimited amount of time with no change requirement. This finding was noted in the prior IT audit.
- DHHS did not have password parameters enabled for the ACTS application. In addition, super users had access to a table within the ACTS application that was not encrypted.

Strong complex password settings and encrypted tables reduce the risk of an unauthorized user gaining access to confidential information and key financial data.

> We recommend password complexity requirements be implemented. In addition, sensitive tables should be encrypted within the application.

8. Physical Security and Environmental Controls

An entity's information resources include computer hardware, peripheral devices, data storage media, and information systems documentation. Physical access to such resources makes it possible for the user to view, use, damage, or misappropriate these resources. Accordingly, such physical access should be restricted to authorized personnel.

- The State Treasurer KidCare programmers had access to the datacenter. Management has accepted the risk based on the size of the IT department.
- NDE controlled access to the DDS datacenter by numeric keypad; however, the pin number was shared by personnel and was not periodically changed.
- Three individuals with access to the DHHS server room did not require the access as part of their job responsibility. This finding was noted in the prior IT audit.
- NPERS did not monitor access to the datacenter. NPERS has obtained bids for controlled access monitoring; however, they have not implemented any changes for fiscal year 2008.

The lack of monitoring access to the datacenter can lead to key financial information being more susceptible to theft, damage, and misuse.

> We recommend only authorized personnel have access to information resources and access to these resources be reviewed on a periodic basis to ensure only authorized individuals have access.

9. Standardized Change Management Process

A formal methodology should be in place to guide the development of applications and systems. Changes to existing applications and systems should undergo initial evaluation, authorization, and implementation procedures to ensure they have met expectations and minimized user disruption.

- The State Treasurer did not have a standard process to implement and track Wagers application changes. The Wagers application did not utilize a separate testing environment to test modifications prior to being implemented into production. Documentation for testing of the Wagers application changes was not maintained. The State Treasurer also did not have a formalized process to test Windows patches and network changes. This finding was noted in the prior IT audit.
- The Department of Roads had not implemented a standard and consistent change control process for database, application, and network modifications. The Department of Roads relied on informal methods of communicating change requests and requirements. Also, a formalized windows patch management process had not been implemented. This finding was noted in the prior IT audit.
- NDE had not developed a formalized process to track changes to the GMS and DDS applications and the databases which support the application. Test plans related to GMS were not documented or retained to ensure the testing of changes prior to migration into production. There was no formal test plans to test changes to the GMS application, until May 2008, when NDE started using a testing protocol for acceptance testing. NDE also did not have a formalized process to test Windows patches. These findings were noted in the prior IT audit.
- DHHS did not have a formalized process to track changes related to the WIC application to ensure all changes were tested and approved by management. In addition, four of five changes to the ACTS application tested did not have formalized documentation on file to ensure changes were appropriate.
- The Office of the CIO did not have a consistent process in place for tracking changes related to the CSB and PACE applications. As of June 2008, the Office of the CIO is in the process of implementing a standard process for all changes.
- The Department of Revenue did not have a standard and consistent change control process for software modifications in place for the entire fiscal year. A new process was implemented in April 2008 however; the process did not include approving changes prior to migration into production. Test documentation for the Motor Fuels application modification was not retained to support the change functioned according to management's intentions and changes were tested in the production environment.

Without proper and consistent change control standards, changes to systems may be made without specific approvals. Without adequate testing, application modifications may not function according to user requests or management's intentions. This could lead to data loss, loss of financial data integrity, and decreased financial data reliability.

> We recommend a standardized change management process be developed and implemented for application and systems changes. The process should include documented change requests, approvals, testing procedures, and approval to implement the change into production. In addition, all modifications to application systems should be tested in an environment separate from the production processing environment.

10. System Monitoring

Computer systems should be adequately monitored to verify they are operating according to management's expectations.

- All recommended system events within the NIS AS/400 were logged; however, there was no periodic review of the logs by the NIS support staff.
- The State Treasurer's office did not have procedures to review the activity in the audit logs within Wagers to ensure transactions were appropriate. The State Treasurer identified an audit log function which can be obtained from the Wagers vendor periodically and reviewed; however, the audit log report had not been requested from Wagers.
- The Department of Roads logged Windows operating system events and security violation reports for invalid logons to the Windows network; however, the logs were not periodically reviewed. This finding was noted in the prior IT audit.
- NDE did not monitor processing performed on the GMS servers. NDE had Windows Audit Policy logs turned on; however, there was no periodic review of the logs for exceptions. This finding was noted in the prior IT audit.
- DHHS did not log security events, super user access, or access to sensitive data within the ACTS application.
- The Department of Revenue did not have procedures to document the review of network activity.

Without monitoring and reviewing data logs to ensure processing occurred successfully, there is an increased risk unauthorized, incomplete, or inaccurate processing will go undetected. Without monitoring security violation reports unauthorized users could access sensitive financial data on the network and financial applications without being detected.

> We recommend a monthly review of critical security events for unauthorized access and inappropriate changes be conducted. We also recommend the review of audit logs and violation reports.

11. Reconciliation and Payment Processes

Good internal control requires a plan of organization, procedures, and records designed to provide reliable financial information. Without a timely and complete reconciliation of records, there is an increased risk for fraud and errors to occur and remain undetected. Good internal control also requires procedures to ensure payments are made only once and paid to the correct individual or vendor.

- The employee who reviews the automated reconciliation between GMS and NIS also processes GMS payments. In addition, GMS did not have appropriate edit checks in place to prevent a user from re-submitting a payment batch. Management has accepted the risk related to the reconciliation process and re-submitting batches. A similar finding was noted in the prior IT audit.

- Disability and Determination Services did not have formal procedures in place to reconcile DDS and NIS and to document the preparation and approval of the reconciliation.
- Labor's reconciliation process did not adequately ensure all cleared checks were properly recorded in the BPS application. This finding was noted in the prior IT audit.
- DHHS did not have appropriate edit checks within the HEA application to ensure only one member of any household received energy payments.
- Claims processed and paid by the State Treasurer did not have adequate documentation on file for the payment of Unclaimed Property. The State Treasurer also did not require individuals who had previously been paid a claim to provide additional proof of ownership for other claims, regardless of the amount of the claim. Proof of ownership must be obtained prior to the payment information being sent to NIS and claims paid. This finding was noted in the prior IT audit.

The reconciliation process may identify either reconciling items or discrepancies requiring adjustment. Recording checks disbursed without reconciliation to the bank balance could result in transactions not being accurately or completely recorded. Ineffective reconciliation procedures may not detect human errors or financial reporting balancing issues. Without adequate system controls in place, there is an increase risk that more than one energy assistance payment could be made to the same household. Without confirming proof of ownership, property may be disbursed to unintended individuals.

> We recommend a formal reconciliation process be implemented to ensure all transactions are accounted for and properly recorded. Automated controls could be established to prevent claims without proper documentation from processing and payments to the same household. We also recommend claims for unclaimed property be supported by proofs of ownership.

12. <u>Business Continuity</u>

Good internal controls require a formalized, tested plan of procedures and organization designed to safeguard assets and minimize the risk data is lost.

- DAS had not fully tested the Continuity of Operations Plan (COOP), which included a disaster recovery plan to relocate critical systems in the event of a disaster.
- NDE did not have adequate procedures to ensure essential business processes and information systems can be recovered timely. NDE has not tested the GMS backup tapes to ensure their completeness, and has not developed a formalized business continuity plan. Additionally, the backup tapes for the DDS application were stored at another building across the street.

When tested comprehensive continuity plans are not in place and tapes are not tested, there is an increased risk for the loss of data.

> We recommend backups are tested and taken offsite to ensure data retention is effective and also to develop a tested comprehensive business continuity plan.

13. Nebraska Lottery Findings

Good internal control requires general computer controls to be in place to reduce the risk of lost or incorrect financial data due to error, fraud, or an unforeseen event.

The Nebraska Lottery had an outside review performed on the applications for on-line vendor (LOTOS), instant ticket vendor (IPS), and Lottery's ICS in May 2006. Nebraska Lottery has remediated several findings since the review. For the findings that have not been remediated, Nebraska Lottery has accepted the risk for issues including, system configurations, business contingency planning, performance monitoring tools, problem management procedures, and segregation of duties. These concerns have been reported in prior Lottery audits.

Without general computer controls in place there is an increased risk of lost or incorrect financial data.

> We recommend the Nebraska Lottery continue to consider these risks in the future and implement necessary controls when needed.

We appreciate and thank all employees involved in the Information Technology examination for their cooperation and courtesy extended to our staff during the engagement.

Sincerely,

Signed Original on File

Mike Foley
State Auditor